IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

HOKKY TJAHJONO, individually and on behalf of all others similarly situated, Plaintiff, v. WESTINGHOUSE AIR BRAKE TECHNOLOGIES CORPORATION, d/b/a WABTEC CORPORATION, Defendant.	Case No. 2:23-cv-531 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Hokky Tjahjono ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendant Westinghouse Air Brake Technologies Corporation, d/b/a Wabtec Corporation ("Wabtec" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against Wabtec for its failure to properly secure and safeguard protected personally identifiable information, including without limitation, individuals' full names, dates of birth; non-US national ID numbers; non-US social insurance numbers or fiscal codes; passport numbers; IP addresses, Employer Identification Numbers; USCIS or Alien Registration Numbers; medical records and health insurance information; photographs; gender; and gender identity; salary; Social Security Numbers; financial account information; payment card information; account usernames and passwords; biometric information;

race and ethnicity; criminal convictions and offenses; sexual orientation; religious beliefs; and union affiliation (collectively, "PII"), for failing to comply with industry standards to protect information systems that contain PII, and for failing to provide timely notice of the breach to Plaintiff and Class. Plaintiff seeks, among other things, damages, and orders requiring Wabtec to adopt reasonably adequate security practices and safeguards to prevent incidents like the unauthorized access from occurring in the future and for Wabtec to provide identity theft protective services to Plaintiff and Class Members for their lifetimes, as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of Wabtec described herein.

2. Wabtec is a wildly successful manufacturer, "producing state-of-the-art locomotives and rail systems."[1] "The firm's 2021 financial results give a revenue figure of $7.8 billion, reporting a staggering 20% of the world's freight being moved by the 23,000 of Wabtec's locomotives in global operation."[2]

3. On or about December 30, 2022, Wabtec announced that it had been the subject of a successful ransomware attack that impacted sensitive information contained on the affected computer systems (the "Data Breach").[3]

4. Based on public information available to date, the information impacted by the Data Breach includes a wide swath of personal information, including individuals' full names, dates of birth; non-US national ID numbers; non-US social insurance numbers or fiscal codes; passport numbers; IP addresses, Employer Identification Numbers; USCIS or Alien Registration Numbers;

---

[1] Bill Toulas, *Rail Giant Wabtec Discloses Data Breach After Lockbit Ransomware Attack*, BleepingComputer (Jan. 3, 2023), https://www.bleepingcomputer.com/news/security/rail-giant-wabtec-discloses-data-breach-after-lockbit-ransomware-attack/.

[2] *Id.*

[3] *Data Security Incident Update – Personal Data Breach Public Communication*, Wabtec (Dec. 30, 2022), https://www.wabteccorp.com/data-security-incident-update-personal-data-breach-public-communication ("Data Breach Notice").

medical records and health insurance information; photographs; gender; and gender identity; salary; Social Security Numbers; financial account information; payment card information; account usernames and passwords; biometric information; race and ethnicity; criminal convictions and offenses; sexual orientation; religious beliefs; and union affiliation.[4]

5. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of cybercriminals who have leaked Plaintiff's and Class Members' PII onto the internet.

6. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

7. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard PII in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future and for Defendant to provide identity theft protective services to Plaintiff and Class Members for their lifetimes.

[4] *Id.*

PARTIES

8. Plaintiff Tjahjono is an adult who at all relevant times is a resident and citizen of the State of Texas. Plaintiff was an employee of Defendant and received a Data Breach Notice from Defendant informing him that his PII had been exposed during the Data Breach

9. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII—time which he would not have had to expend but for the Data Breach.

10. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

11. Defendant Wabtec is a Delaware corporation with a principal place of business located at 30 Isabella Street, Pittsburgh, Pennsylvania 15212. Defendant Wabtec operates under the fictious name, Wabtec Corporation.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

13. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

14. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

FACTUAL BACKGROUND

15. Wabtec is the "world's foremost rail technology company," leading "the way in creating a more sustainable freight and passenger transportation network."[5]

16. Wabtec employs over 27,000 employees in over 50 counties around the world.[6]

17. During individuals' course of employment with Wabtec, Defendant receives, creates, and handles PII, which includes, *inter alia*, individuals' full names, dates of birth; non-US national ID numbers; non-US social insurance numbers or fiscal codes; passport numbers; IP addresses, Employer Identification Numbers; USCIS or Alien Registration Numbers; medical records and health insurance information; photographs; gender; and gender identity; salary; Social Security Numbers; financial account information; payment card information; account usernames and passwords; biometric information; race and ethnicity; criminal convictions and offenses; sexual orientation; religious beliefs; and union affiliation.

18. In order to work for Wabtec, employees must entrust their PII to Defendant, and in return, they reasonably expect that Defendant will safeguard their highly sensitive PII.

19. Even though Wabtec "is committed to and takes very seriously its responsibility to safeguard all data entrusted to it,"[7] Wabtec nevertheless employed inadequate data security measures to protect and secure the PII employees entrusted to it, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII.

---

[5] *About Wabtec*, Wabtec, https://www.wabteccorp.com/about-wabtec (last visited Jan. 6, 2023).
[6] *Id.*
[7] *Data Breach* Notice, *supra* note 3.

A. The Value of Private Information and Effects of Unauthorized Disclosure.

20. Wabtec was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

21. Wabtec also knew that a breach of its computer systems, and exposure of the PII stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

22. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

23. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[8]

24. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[9]

25. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[10]

---

[8] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[9] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

[10] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

26. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[11]

27. The ramifications of Wabtec's failure to keep Plaintiff and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[12]

28. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

---

[11] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Jan. 6, 2023).

[12] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 6, 2023).

29. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's employees especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

30. Based on the value of its employees PII to cybercriminals, Wabtec knew or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. Wabtec failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

B. Manufacturing Companies are Particularly Vulnerable to Data Breaches.

31. Wabtec also knew or should have known that manufacturing companies, such as itself, have become prime targets for cybercriminals.

32. "As an industry, manufacturers are one of the least technology mature industries, regularly outpaced by companies in media, finance and healthcare. Among global manufacturers, only 24% have implemented a smart manufacturing initiative, and just another 22% are in the pilot stages. That leaves more than half of global manufacturers relying on systems and processes that haven't kept up with modern security measures."[13]

33. "This lagging security expertise, combined with a low tolerance for disruption, has set up manufacturers to be rising targets for cybercriminals."[14]

[13] Cathy Pitt, Why Cybercriminal Target Manufacturers – And What to do About it, Security https://www.securitymagazine.com/articles/94030-why-cyber-criminals-target-manufacturers-and-what-to-do-about-it (last visited Jan. 6, 2023).
[14] *Id.*

34. Indeed, IBM's annual X-Force Threat Intelligence Index reported that the manufacturing sector was the most targeted industry for cyberattacks in 2021, dethroning the financial services and insurance industry as the most attacked industry.[15]

35. Cybercriminals have further targeted manufacturing companies in part because of the critical role these companies play in the global supply chain and because successful attacks against manufacturing companies immediately create problems in the production and supply chain, making it more likely that cybercriminals can demand lucrative ransoms.[16]

36. Put differently, cybercriminals target the manufacturing industry because disrupting the supply chain "strikes at the heart of a manufacturer's ability to meet customer orders and grow revenue. Many manufacturers quietly pay the ransom because they have no other choice."[17]

C. Defendant Breached its Duty to Protect its Employees' PII.

37. On June 26, 2022, Wabtec detected unusual activity on its network leading to an investigation of the attack and whether the hackers had exfiltrated any data.[18]

[15] Chris Ehrilich, *Manufacturing is the 'Most Targeted' Industry for Cyber Attacks*, Datamation (Mar. 9, 2022), https://www.datamation.com/security/manufacturing-most-targeted-industry-cyber-attacks/.
[16] *Manufacturing Sector is the Most Popular Target of Cyber* Attacks, Cybersec Europe (Mar. 21, 2022), https://www.cyberseceurope.com/blog/artikel/manufacturing-sector-is-the-most-popular-target-of-cyber-attacks/.
[17] Louis Columbus, *The Manufacturing Industry's Security Epidemic Needs a Zero-Trust Cure*, Venture Beat (Nov. 15, 2022), https://venturebeat.com/security/the-manufacturing-industrys-security-epidemic-needs-a-zero-trust-cure/.
[18] *Data Breach Notice*, *supra* note 3.

38. The next day, news outlets reported that sources at one of Wabtec's manufacturing plants indicated that it was a ransomware attack impacting the rail giant. However, the company did not official respond to the rumors.[19]

39. Wabtec subsequently discovered that on or about March 25, 2022, cybercriminals had introduced malware into certain Wabtec systems.[20]

40. On or about November 23, 2022, Wabtec concluded its investigation and determined that certain systems containing personal information were subject to unauthorized access.[21] Wabtec further determined that personal information contained in the impacted systems was exfiltrated by cybercriminals.[22]

41. The information impacted by the Data Breach includes a wide swath of personal information, including individuals' full names; dates of birth; non-US national ID numbers; non-US social insurance numbers or fiscal codes; passport numbers; IP addresses; Employer Identification Numbers; USCIS or Alien Registration Numbers; medical records and health insurance information; photographs; gender; and gender identity; salary; Social Security Numbers; financial account information; payment card information; account usernames and passwords; biometric information; race and ethnicity; criminal convictions and offenses; sexual orientation; religious beliefs; and union affiliation.[23]

---

[19] Lisa Adams, *Possible Ransomware Attack Allegedly Impacted Wabtec*, Erie News Now (June 27, 2022), https://www.erienewsnow.com/story/46773012/possible-ransomware-attack-allegedly-impacting-wabtec.
[20] Toulas, *supra* note 1.
[21] *Id.*
[22] *Id.*
[23] *Data Breach Notice*, *supra* note 3.

42. While Wabtec has not indicated the cybercriminals responsible for the Data Breach, the ransomware group, LockBit, has claimed responsibility for the Data Breach.[24]

43. A few weeks after news outsets reported that Wabtec was subject to a possible ransomware attack, LockBit published samples of data stolen from Wabtec on its ransomware website.[25]

44. LockBit demanded that Wabtec pay up to $30 million dollars for the decryptor and to destroy the stolen documents.[26] After Wabtec presumably refused to pay the ransom, LockBit leaked all of the solen data on its ransomware website on or about August 20, 2022.[27]

45. The data posted on LockBit's disclosure site, identified as belonging to Wabtec, appears to be a combination of internal employee PII, partner/customer invoices, and non-employee PII data.[28]

46. Following the publishing of the exfiltrated data on LockBit's ransomware site, Wabtec waited approximately four additional months and began notifying affected Class Members, including Plaintiff, of the Data Breach on or around December 30, 2022. [29]

47. While Wabtec has not released the total number of individuals impacted by the Data Breach, Wabtec employees approximately 27,000 persons, and upon information and belief thousands of individuals were impacted by the Data Breach.[30]

---

[24] Toulas, *supra* note 1.
[25] *Id.*
[26] Prajeet Nair, Wabtec Discloses Data Breach; LockBit Claims Responsibility, Bank Info Security (Jan 4, 2023), https://www.bankinfosecurity.com/wabtec-discloses-data-breach-lockbit-claims-responsibility-a-20853.
[27] Toulas, *supra* note 1.
[28] Steve Zurier, *Wabtec Breach Linked to LockBit Ransomware Group*, SC Media (Jan 4, 2023), https://www.scmagazine.com/news/ransomware/wabtec-breach-linked-to-lockbit-ransomware-group.
[29] *Data Breach Notice*, *supra* note 3.
[30] Toulas, *supra* note 1.

48. The Data Breach is the direct and proximate result of Wabtec's failure to implement reasonable data security measures to protect the PII in its custody.

D. FTC Guidelines Prohibit Wabtec from Engaging in Unfair or Deceptive Acts or Practices.

49. Wabtec is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

50. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

51. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[32]

52. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

[31] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[32] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformationpdf.

on the network; and verify that third-party service providers have implemented reasonable security measures.[33]

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

54. Wabtec failed to properly implement basic data security practices. Wabtec's failure to employ reasonable and appropriate measures to protect against unauthorized access to student PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

55. Wabtec was at all times fully aware of its obligations to protect the PII of students because of its position as an institution of higher education, which gave it direct access to reams of student PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Plaintiff and Class Members Suffered Damages.

56. The ramifications of Wabtec's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Plaintiff and Class Members now face years of constant surveillance of their personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

57. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class

[33] *Id.*

Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff and Class Members' PII has been diminished by its exposure in the Data Breach.

58. Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII as a result of the Data Breach. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[34]

59. Besides the monetary damage sustained in the event of identity theft, Plaintiff and Class Members may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[35]

60. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its users' PII.

61. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers.

---

[34] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Jan. 6, 2023).

[35] Kathryn Parkman, *How to Report identity Theft*, ConsumerAffairs (Feb. 17, 2022), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html.

62. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including out of pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their PII being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their PII; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to it.

CLASS ALLEGATIONS

63. Plaintiff brings this class action on behalf of himself and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

64. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the Wabtec Data Breach which was announced on or about December 30, 2022 (the "Class").

65. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

66. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

67. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes thousands of individuals.

68. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

69. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all employees of Defendant, each having their PII exposed and/or accessed by an unauthorized third party.

70. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained

counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

71. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

72. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

73. **Injunctive Relief –** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

74. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

75. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

76. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' PII in Defendant's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

77. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by cyber-criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

78. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's

and Class Members' PII in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

79. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

80. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of cyber-criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protected Plaintiff.

81. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

82. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

83. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by institutions such as Defendant or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

84. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach within the higher education sector.

85. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

86. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

87. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

88. As a direct and proximate result of Defendant's negligence, Plaintiff's and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

89. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

90. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

91. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Wabtec is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Wabtec's data security measures remain inadequate,

Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

92. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Wabtec owes a legal duty to secure employees' PII and to timely notify employees of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. Wabtec continues to breach this legal duty by failing to employ reasonable measures to secure employees' PII.

93. This Court also should issue corresponding prospective injunctive relief requiring Wabtec to employ adequate security protocols consistent with law and industry standards to protect employees' PII.

94. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Wabtec. The risk of another such breach is real, immediate, and substantial. If another breach at Wabtec occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

95. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Wabtec if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Wabtec of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Wabtec has a pre-existing legal obligation to employ such measures.

96. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Wabtec, thus eliminating the additional injuries that would result to Plaintiff and employees whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: March 27, 2023

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch
Kelly K. Iverson
Nicholas A. Colella
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
P: (412) 322-9243
gary@lcllp.com
kelly@lcllp.com
nickc@lcllp.com

Attorneys for Plaintiff